IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-27,

Defendants.

Civil Action No. 1:10cv0156 (LMB/JFA)

PROPOSED FINDINGS OF FACT AND RECOMMENDATIONS

This matter is before the court on plaintiff's second motion for default judgment pursuant to Federal Rule of Civil Procedure 55(b)(2). (Docket no. 84). In this action, the plaintiff, Microsoft Corporation ("Microsoft"), seeks a default judgment ordering that the registry for 276 domain names transfer the registrations for those domain names to a specified registrar who will then transfer the registrations for those domain names to Microsoft. Pursuant to 28 U.S.C. § 636(b)(1)(C), the undersigned magistrate judge is filing with the court his proposed findings of fact and recommendations, a copy of which will be provided to all interested parties.

Procedural Background

On February 22, 2010, Microsoft filed its Complaint against 27 John Doe registrants of 273 domain names alleging that the defendants had used the domain names in conjunction with the creation of a malicious botnet known as the Waledac Botnet. (Docket no. 1). That same day, Microsoft filed a motion to seal the case (Docket no. 3), an Application for an Emergency Temporary Restraining Order and Order to Show Cause re a Preliminary Injunction ("Application") (Docket nos. 4, 5). The Application was supported by declarations of Andre M. Dimino (Docket no. 6), Dean Turner (Docket no. 7), David Dittrich (Docket no. 8), T.J.

Campana (Docket no. 9), and Gabriel M. Ramsey (Docket no. 10) and by a memorandum in support (Docket no. 11). Microsoft also filed a Supplemental Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction on February 22, 2010. (Docket nos. 14, 15). The supplemental application was supported by a memorandum in support (Docket no. 16) and by a declaration of T.J. Campana (Docket no. 17).

On February 22, 2010, the District Judge held a hearing on Microsoft's Application and supplemental application (Docket no. 19) and entered an Order sealing this matter for three business days (Docket no. 12) as well as an Order temporarily restraining and enjoining defendants from engaging in activities related to the Waledac Botnet (Docket no. 13). The District Judge ordered that the registry of the domain names at issue, VeriSign, Inc. ("VeriSign"), immediately lock the domains at the registry level and hold them in escrow. (Docket no. 13). The Order also set a hearing on the request for a preliminary injunction for March 8, 2010 at 9:00 a.m. and required Microsoft to serve the defendants by any means authorized by law, including: (1) personal delivery upon defendants who provided contact information in the United States; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China; (3) transmission by e-mail, facsimile and mail to the contact information defendants provided to their respective domain name registrars and as agreed to by defendants in their domain name registration agreements; and (4) publishing a notice of these proceedings on a publicly available Internet website. *Id.* The Order set a bond in the amount of $54,600.00, which Microsoft deposited with the court that same day. (Docket no. 18). A second Order of February 22, 2010 added four additional domain names that were not named in the complaint or the initial application for the temporary restraining order. (Docket no. 27). Pursuant to that Order, Microsoft deposited an additional bond in the amount of $800.00. (Docket no. 28).

On February 22, 2010, summonses were issued as to the 27 John Doe defendants (Docket nos. 20, 21, 22). Plaintiff filed a motion for a protective order sealing documents (Docket no. 24) and a non-confidential memorandum in support of that motion (Docket no. 25) on February 22, 2010. That motion was granted that same day. (Docket no. 26).

On March 5, 2010, Microsoft filed a status report regarding its motion for preliminary injunction. (Docket no. 32). In its status report, Microsoft described the efforts it had undertaken to serve the defendants. *Id.* It also stated that it no longer sought a preliminary injunction as to the domain "name-services.com" because temporary relief as to that site was not longer necessary to address the injury caused by the Waledac Botnet. *Id.* On March 8, 2010 the hearing on Microsoft's application for a preliminary injunction was held before the District Judge (Docket no. 33) and on March 10, 2010 an Order was entered granting Microsoft's request for a preliminary injunction enjoining certain activities of the John Doe defendants and locking the registrations for 276 domain names (Docket no. 38).

On March 9, 2010, Microsoft filed a Motion for Limited Authority to Conduct Discovery Necessary to Identify and Serve Doe Defendants (Docket no. 34) along with a memorandum in support (Docket no. 35) and noticed it for a hearing on March 19, 2010 (Docket no. 36). On the day of the hearing, no defendant appeared and Microsoft's motion was granted by an Order of March 19, 2010. (Docket no. 40).

Microsoft filed its second status report regarding the preliminary injunction on April 7, 2010. (Docket no. 41). This status report indicated that despite diligent efforts, neither it nor the domain names' registrars had received any communication from any of the registrants. *Id.*

Microsoft also noted that it had served a number of subpoenas on third parties believed to possess information relevant to this case. *Id.* Microsoft filed its third status report on July 1, 2010. (Docket no. 42). In that status report, Microsoft further detailed the efforts it undertook to serve the defendants pursuant to the court's Orders of February 22, 2010. *Id.*

On July 12, 2010, Microsoft filed its request for entry of default (Docket no. 43) and motion for default judgment (Docket no. 46). It also filed a combined memorandum in support of the request for entry of default and motion for default judgment (Docket no. 47) along with declarations from Gabriel Ramsey (Docket no. 48) and T.J. Campana (Docket no. 49). Microsoft noticed the motion for default judgment for a hearing on August 6, 2010 (Docket no. 50). Microsoft also filed a motion to seal portions of T.J. Campana's declaration and an exhibit attached thereto (Docket no. 44) with a memorandum in support (Docket no. 45) and a notice setting a hearing on that motion for August 6, 2010 (Docket no. 51). On August 5, 2010, Microsoft filed a supplemental brief in support of its request for entry of default and motion for default judgment (Docket no. 52) and supplemental declaration of Gabriel M. Ramsey (Docket no. 53). On August 6, 2010, a hearing was held on the motions. (Docket no. 55). That same day, an Order was entered granting Microsoft's motion for entry of default (Docket no. 54) and another Order was entered denying without prejudice Microsoft's motion for default judgment (Docket no. 56). The Clerk entered a default as to each defendant on August 6, 2010, with the exception of one default which was entered on August 12, 2010.[1] (Docket nos. 58-83, 87).

On August 10, 2010, Microsoft filed its Renewed Motion for Default Judgment (Docket no. 84) with a declaration of Gabriel M. Ramsey (Docket no. 85) and noticed that motion for a hearing on September 3, 2010 at 10:00 a.m. (Docket no. 86). On September 3, 2010 at 10:00

[1] The Clerk inadvertently failed to enter default as to John Doe number 19 on August 6, 2010. This oversight was corrected on August 12, 2010. (Docket no. 87).

a.m., counsel for Microsoft appeared and presented argument on its renewed motion and no one appeared on behalf of any of the defendants. (Docket no. 88).

Factual Background

The following facts are established by the Complaint (Docket no. 1) ("Compl."), the Application for an Emergency Temporary Restraining Order and Order to Show Cause re a Preliminary Injunction (Docket no. 4) and the Brief in Support of Microsoft's Motion for Default Judgment (Docket no. 47). Plaintiff Microsoft is a corporation organized under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington. (Compl. ¶ 2). Microsoft is a provider of the Windows® operating system, Hotmail® e-mail services and a variety of other software and services, and has invested substantial resources in developing its products and services. *Id.* ¶ 20. Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows® and Hotmail® marks. *Id.*

The defendants are 27 individuals or entities ("Doe Defendants") that control 273 harmful Botnet domains ("Botnet Domains") which Microsoft alleges are being misused to cause harm to Microsoft, its customers and the public. *Id.* ¶ 3. Microsoft is unaware of the true names and capacities of the Doe Defendants and therefore sued the Doe Defendants by fictitious names. *Id.* ¶ 4. The Doe Defendants own, operate, and control the Waledac Botnet and do business under the names of the Botnet Domains. *Id.*

In general, a "botnet" is a collection of individual computers, each running software that allows communication among those computers and allows centralized or decentralized communication with other computers providing control instructions. *Id.* ¶ 21. The individual computers in a botnet often belong to individual users who have unknowingly downloaded or been infected by the software that makes the computer part of the botnet. *Id.* A user's computer may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment or downloads fraudulent software. *Id.* In each such instance, software code is downloaded or executed on the user's computer, causing that computer to become part of the botnet, capable of sending and receiving communications, code, and instructions to or from other botnet computers. *Id.* Some botnet computers, referred to as "command and control" computers, are wholly within the control of the botnet creator and may have specialized functions, such as sending control instructions. *Id.* ¶ 22.

Botnets are often used to carry out misconduct that harms others' rights. *Id.* ¶ 23. For example, a computer in a botnet may be used to send anonymously unsolicited, bulk email without the knowledge or consent of the individual user who owns the compromised computer. *Id.* Similarly, a botnet computer may be used to deliver further malicious software that infects other computers, making them part of the botnet as well. *Id.* A botnet computer may also be used to carry out fraud, computer intrusions, and other misconduct or to "proxy" or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications. *Id.*

The Waledac Botnet has a multi-tiered architecture. *Id.* ¶ 25. The lowest "Spammer Node" tier in this architecture is made up of infected user computers that have been determined to be behind firewalls or otherwise not directly accessible from the Internet. *Id.* ¶ 26. The botnet software placed on these infected computers sends, without the user's knowledge or permission, unsolicited bulk email (often known as "spam"). *Id.* This spam email may contain code that infects further computers adding them to the botnet or may serve other purposes, such as inviting users to enter financial or other valuable personal information. *Id.* The sending of spam email is a major component of the Waledac Botnet's functionality. *Id.* The Waledac Botnet operators sell botnet capacity as a service, including the capability of sending spam email to perpetuate fraud, to collect financial and personal data and to distribute harmful or fraudulent software, including fake antivirus or "scareware" programs. *Id.*

The next highest tier in the architecture, the "Repeater Node" tier, is made up of infected computers that are directly accessible from the Internet. *Id.* ¶ 27. These computers may serve several different purposes, such as acting as proxies relaying communications among different botnet computers, acting as HTTP and SOCKS 5 servers capable of delivering HTTP and SOCKS 5 commands and responses and acting as "DNS servers." *Id.* In general, a DNS server is a computer that translates human readable hostnames or domain names (such as xinnet.com) to their corresponding binary identifier, called an IP address (such as 123.100.5.81). *Id.*

The next highest tier in the architecture, the "TSL Servers," is the first tier that is controlled directly by the operators of the Waledac Botnet and the first tier that is not made up of infected computers. *Id.* ¶ 28. The TSL Servers are "reverse proxy servers," which receive in-bound communications and then pass those on to additional servers. *Id.* In the Waledac Botnet, the TSL Servers receive in-bound communications from the Repeater Nodes and then pass them to other servers behind the TSL Servers. *Id.* The purpose of TSL Servers is to obfuscate details about the servers behind them, to prevent direct communications with those servers and evade investigation of those portions of the botnet. *Id.*

At the highest level, behind the TSL Servers, there are one or more command and control servers, referred to as the "Main Command & Control" servers, which are also controlled directly by the operators of the Waledac Botnet and are not made up of infected computers. *Id.* ¶ 29. The Main Command & Control servers are responsible for coordinating the Waledac Botnet on the whole and providing the most fundamental definitions, commands, and instructions that determine how infected computers will operate and how different botnet components will interact with each other. *Id.*

The Waledac Botnet uses a method called "fast flux" hosting, which is a technique used by botnets to hide the location of their constituent computers by constantly changing the addressing of the domain names that are associated with the command and control and infrastructure components that make up the botnet. *Id.* ¶ 30. The purpose and result of fast flux hosting is that discovery, observation and counter-measures are made more difficult because the addressing of the constituent compromised computers is constantly changing. *Id.*

The Waledac Botnet includes a component called the "Fast Flux DNS Server," which coordinates the domain name infrastructure associated with the Repeater Nodes thereby using a fast flux hosting technique to hide the source, location, owner, and other attributes of those computers. *Id.* ¶ 31. The Fast Flux DNS Server accomplishes this by regularly updating the root name servers for the various fast flux domains used by the Waledac Botnet. *Id.* In particular, the Fast Flux DNS Server accesses a web portal to one of the domains' registrars updating the root name servers at the registrars. *Id.* To hide the location of the Fast Flux DNS Server from the registrars, all access of the server to the registrar's web portal is proxied through Repeater Node computers so there is no direct communication between the Fast Flux DNS Server and the registrar. *Id.* The botnet's Fast Flux DNS Server can instruct a subset of the Repeater Nodes to act as DNS servers while the Fast Flux DNS Server reconfigures the root DNS servers to point to the configured nodes. *Id.* As a result, a query by a computer to one of the Waledec domain names results in one of the Repeater nodes responding with the IP address of the queried computer or another Repeater Node computer, thereby providing the ability to continuously obscure the attributes of these Waledac domains. *Id.* Each of the Botnet Domains listed in Appendix A to the complaint is alleged to be one of the foregoing described fast flux Waledac domains, representing a component in the command and control of the botnet. *Id.* ¶ 32.

The computers that are part of the Waledac Botnet can send "node table updates" to other computers in the botnet. *Id.* ¶ 33. These node table updates contain lists of other known Repeater Nodes, to enable and support continued communication between all of these computers. *Id.* The communication from the Spammer Node tier to the Repeater Node tier and communication between Repeater Nodes depends on the accuracy of the node tables stored at each computer and depends on the accuracy of node table updates. *Id.* If a node table is empty or contains invalid entries, a given botnet computer uses one of the Botnet Domains, which is hard coded in the botnet software residing on the computer, to query the botnet for an update to the node table. *Id.* Thus, the Botnet Domains continuously control the ability of the computers that makeup the Waledac Botnet to communicate with each other and to grow the botnet. *Id.*

In addition to supporting Waledac Botnet's infrastructure, the Botnet Domains may be used by including links to those domains in unsolicited, bulk email sent out by Spammer Node computers with the purpose of spreading the botnet. *Id.* ¶ 34. For example, the Spammer Node computers have been observed to send emails indicating to the victim recipients that a news story has broken or that a loved one has sent the victim an e-card. *Id.* The emails point to one of the Botnet Domains, which represents a Repeater Node computer. *Id.* When the victim opens the link sent to them, in order to retrieve the story or e-card, the victim is interacting directly with the Repeater Node computer, which may deliver software that infects the victim's computer and makes it part of the Waledac Botnet. *Id.*

The Waledac Botnet software is maliciously introduced onto users' computers, infecting those computers and making them part of the botnet. *Id.* ¶ 35. These acts constitute an unauthorized intrusion into the Microsoft Windows operating system which Microsoft licenses to the end users. *Id.* In particular, the Waledac Botnet specifically targets the Windows operating system. For example, the Waledac Botnet writes particular entries to the registry of the Windows operating system, without the consent of Microsoft or its customers, including: commands that tell the computer which commands to execute; commands that facilitate communication between botnet computers; commands that harvest personal email addresses from the computer; commands that tell the computer how to receive instructions from the botnet operator; and data identifying the computer within the botnet. *Id.* The spread of the Waledac Botnet in this way is achieved by misleading unwitting users into taking steps that result in the infection of their machines. *Id.*

The Waledac Botnet's intrusion into Microsoft's Windows operating system is without the authority of Microsoft and exceeds any authority granted by Microsoft to any third party, including the end-user and the operators of the Waledac Botnet. *Id.* ¶ 36. The Waledac Botnet harms Microsoft's customers by misusing the Windows operating system on those users' infected computers. *Id.* ¶ 37. The Waledac Botnet causes harm to Microsoft's customers by, among other things, causing customers' computers to: (i) install and run software without the customers' knowledge or consent, including software to support the botnet infrastructure, software that causes the computer to act as an HTTP Proxy, an HTTP Server, a DNS Server, a

SOCKS 5 Proxy, software that acts as an SMTP email engine, software enabling the computer to initiate a DDoS attack, and an HTTP P2P Engine; (ii) install and run fake anti-virus software and other similar software; (iii) have deteriorated performance due to the running of unauthorized software; (iv) install and run software without the customers' knowledge and consent which collects personal information, including personal email address information of the customers and others; (v) send spam email to others, including users of Microsoft's Hotmail email account holders and users of Microsoft's Outlook email program; (vi) send spam email falsely appearing to originate from Microsoft's Hotmail email service; and (vii) transmit collected personal information, including personal email address information to the Waledac Botnet Main Command & Control Server. *Id.* ¶ 37. For example, Microsoft recently conducted an analysis of spam email originating from the Waledac Botnet and learned that in an 18 day period the botnet attempted to send over 651 million emails to Microsoft's Hotmail users and was able to cause between 700,000 and 2.5 million emails per day to reach those users. (Docket no. 9 ("Campana Decl.") ¶¶ 32-41).

The unauthorized access of and intrusion into Microsoft's Windows operating system and Microsoft's customers' computers results in consumer confusion. (Compl. ¶ 38). Microsoft's customers have notified Microsoft of damage caused by the Waledac Botnet and the Botnet Domains. *Id.*; *see also* (Campana Decl. ¶¶ 19-31). Customers have been confused and have been incorrectly led to believe that Microsoft was the source of damage and therefore attributed their injury to Microsoft and its products and services. (Compl. ¶ 38). This incorrect attribution of the effects of the Waledac Botnet and the Botnet Domains to Microsoft causes harm to Microsoft's brand and tarnishes the reputation of Microsoft's name, products, and services. *Id.* Microsoft has had to expend substantial resources in an attempt to assist its customers and to correct the continuing misperception that Microsoft is the source of damage caused by the Waledac Botnet and the Botnet Domains. *Id.* The Doe Defendants who operate the Waledac Botnet benefit from its operation and the activities described above by sending spam email which generates advertising revenue and by selling to others, for profit, the botnet's capability of sending unsolicited, bulk email and carrying out other activities on behalf of others. *Id.* ¶ 39.

Microsoft and its customers are injured when the Waledac Botnet software is maliciously introduced onto users' computers making them part of the botnet. (Campana Decl. ¶¶ 24-31; Docket no. 8 ("Dittrich Decl.") ¶¶ 24-27). These acts constitute an unauthorized intrusion into the Microsoft Windows operating system in which Microsoft retains a possessory interest. (Campana Decl. ¶¶ 24-31, Exs. 6-7; Dittrich Decl. ¶ 24-27). The Waledac Botnet specifically targets the Windows operating system by, among other things, writing particular entries to the registry of the Windows operating system, without the consent of Microsoft or its customers. (Campana Decl. ¶¶ 25-27). Similarly, the botnet installs and runs fake "anti-virus" software under the misleading name "MS Antispyware 2009," which is designed to mislead consumers into installing the software. (Campana Decl. ¶¶ 42-43, Ex. 2 at 30; Dittrich Decl. ¶¶ 24, 31-32). The unauthorized software causes injury by degrading the performance of the user's computer and misleading Microsoft's customers. *Id.*

Proposed Findings and Recommendations

Rule 55 of the Federal Rules of Civil Procedure provides for the entry of a default judgment when "a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend." Based on the failure of the defendants to file a responsive pleading in a timely manner, the Clerk has entered a default as to each defendant. (Docket nos. 58-83, 87). A defendant in default admits the factual allegations in the complaint. *See* Fed. R. Civ. P.

8(b)(6) ("An allegation – other than one relating to the amount of damages – is admitted if a responsive pleading is required and the allegation is not denied."); *see also GlobalSantaFe Corp. v. Globalsantafe.com*, 250 F. Supp. 2d 610, 612 n.3 (E.D. Va. 2003) ("Upon default, facts alleged in the complaint are deemed admitted and the appropriate inquiry is whether the facts as alleged state a claim."). Rule 55(b)(2) of the Federal Rules of Civil Procedure provides that a court may conduct a hearing to determine the amount of damages, establish the truth of any allegation by evidence, or investigate any other matter when necessary to enter or effectuate judgment.

Jurisdiction and Venue

A court must have both subject matter and personal jurisdiction over a defaulting defendant before it can render a default judgment. Microsoft has alleged that this court has subject matter jurisdiction pursuant to the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7704; the Electronic Communications Privacy Act, 18 U.S.C. § 2701; and the Lanham Act, 15 U.S.C. § 1125. As such, this is an action arising under the laws of the United States over which this court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Microsoft has also alleged that the Doe Defendants have committed trespass to chattels, unjust enrichment, and conversion. These allegations are so related to Microsoft's claims under the above cited federal statutes that they form part of the same case or controversy. Thus, this court has subject matter jurisdiction over these claims pursuant to 28 U.S.C. § 1367.

Microsoft has also alleged that the Doe Defendants maintain computers and Internet websites and engage in other conduct availing them of the privilege of conducting business in Virginia, have directed acts complained of in the complaint toward Virginia, and have utilized instrumentalities located in Virginia to carry out the acts. In addition, the registry for the Botnet Domains maintained by the defendants is VeriSign, which is located in the Eastern District of Virginia. Microsoft alleges that it is through the Botnet Domains, by using these Domains to control the communications of the Waledac Botnet and direct malicious computer code, that the Doe Defendants are causing harm to Microsoft, its customers, and the public, including users located within this district.

Microsoft alleges that venue is proper in this judicial district under 28 U.S.C. § 1391(b) because a domain name is deemed to have its situs in the judicial district in which the domain name registry that registered or assigned the domain name is located. Microsoft notes that VeriSign is the domain name registry for the Botnet Domains and is located in this district. Microsoft further alleges that venue is proper because a substantial part of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district.

For these reasons, the undersigned magistrate judge recommends a finding that this court has subject matter jurisdiction over this action, that the court has personal jurisdiction over the Doe Defendants and Botnet Domains, and that venue is proper in this court.

Service

As discussed above, the District Judge entered an Order on February 22, 2010 requiring Microsoft to serve the defendants by any means authorized by law, including: (1) personal delivery upon defendants who provided contact information in the United States;[2] (2) personal

[2] Microsoft personally served Stephen Paluck and Wild West Domains, the registrant and registrar, of the domain <debtbgonesite.com>. Microsoft learned that Mr. Paluck had provided access to that domain to a third party company, but was unable to determine who at that company may have had control over the domain. (Docket no. 32, Ex. 2 at ¶ 4). Microsoft has been working with Mr. Paluck to ensure that his computer is virus free and to determine the true

delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China; (3) transmission by e-mail, facsimile and mail to the contact information defendants provided to their respective domain name registrars and as agreed to by defendants in their domain name registration agreements; and (4) publishing a notice of these proceedings on a publicly available Internet website. (Docket no. 13).

On March 1, 2010, copies of all pleadings and orders in this action were delivered to the Ministry of Justice of the People's Republic of China pursuant to the Hague Convention. (Docket no. 32, Ex. 2, ¶ 30). Microsoft requested that the Ministry of Justice personally serve the documents on the Doe Defendants at the physical addresses provided by the registrants of the Botnet Domains. *Id.* There is no indication that the Ministry has been able to deliver the documents and it is believed that it may take between 3 and 6 months for the Ministry of Justice to attempt personal service. *Id.* Further, investigation by Microsoft's U.S. and China counsel regarding the physical addresses associated with the domains revealed that almost all of the addresses are false. (Docket no. 10 ¶¶ 3-5). The domain registrars in China have also confirmed in their communication with Microsoft's counsel that the physical address information is false. (Docket no. 32, Ex. 2, ¶ 10). Thus physical service does not appear to be possible as to the Doe Defendants who provided contact information in China.

On February 24, 2010, Microsoft provided notice and service of the complaint, summons and related materials in English and Chinese through the publicly available website www.noticeofpleadings.com, and has updated the website throughout this case. (Docket no. 32,

source of the misuse of his domain. *Id.* at ¶ 5. Pursuant to an agreement, Microsoft has compensated Mr. Paluck for the domain and has acquired all actual and beneficial interest in the domain <debtbgonesite.com>. *Id.* While Microsoft now owns the domain, to ensure that the site is not further compromised and for consistent application of relief, Microsoft requests that default judgment be entered as to <debtbgonesite.com>.

Ex. 2, ¶ 16). The court's orders and notice regarding this action have also been widely reported in international media publications, including news media in China. (Docket no. 32, Ex. 2, ¶¶ 15-22). The reporting and publication of this action in China and throughout the world has been continuous. (Docket no. 48, Ex. 11 ("Ramsey Decl.")). There is evidence indicating that Doe Defendants are specifically aware of the www.noticeofpleadings.com website and thus have actual notice of the complaint and pleadings. (Docket no. 47, pages 4-5). Counsel for Microsoft has monitored Internet traffic to the website between late February 2010 and the present. (Ramsey Decl., Exs. 2-5). During that four-month period, beyond the "ordinary" website traffic from a variety of IP addresses (*i.e.*, interested visitors reading the pleadings) and some law enforcement visits, there have been thousands of visits from one particular IP address (212.176.17.62), associated with a company in Moscow. (Ramsey Decl., Ex. 6). This IP address is reported as having been used in the past to carry out distributed denial-of-service attacks on a Russian language investigative journalism website. (Ramsey Decl., Ex. 7). Moreover, this recent traffic to the www.noticeofpleadings.com website has not been confined to merely viewing pages on the site, but has included a series of http requests designed to probe the site for potential security weaknesses. (Docket no. 49 ("Campana Decl.") ¶¶ 4-8, Ex. 1; Ramsey Decl., Ex. 8). In particular, as seen in the error logs for May 2010, a number of requests were made to the website that attempted to locate files that do not exist on the server hosting the website. Among the requested files are "admin_login.asp," "login.asp," "errors.php" and many others. *Id.* Searching for such "login.asp" files or "errors.php" files are common first steps in carrying out website compromise techniques called "SQL Injection" or "PHP Remote File Injection." (*See* Campana Decl., Ex. 1, ¶¶ 4, 6; Ramsey Decl., Exs. 9, 10). Similarly, a visitor to the site was probing directories where active files that could be compromised might be located. (Campana

Decl. ¶ 8). This is strong evidence that the Doe Defendants are not only aware of the lawsuit and the Complaint, but have deliberately accessed the www.noticeofpleadings.com website and are aware of its contents.

Between February 26, 2010 and March 3, 2010, Microsoft sent emails to the email addresses identified in the registrant contact information for the Waledac Botnet Domains. (Docket no. 32, Ex. 2, ¶¶ 23-26). The emails provided service of the complaint, summons and related materials on the Doe Defendants. *Id.* Of the 28 email addresses associated with the Botnet Domains, emails providing initial notice and service were successfully sent to 18 addresses. *Id.* The recipients have not responded to the notice. *Id.* The remaining 10 email addresses were not operational and resulted in error messages when emails were sent to them. *Id.* Microsoft's counsel conducted additional research but has not discovered any other information enabling further contact information associated with the domains. (Docket no. 32, Ex. 2, ¶ 31). Further, Microsoft's counsel in Beijing, China has contacted the Chinese domain registrars through which most of the Botnet Domains were registered. (Docket no. 32, Ex. 2, ¶¶ 9-14; Ramsey Decl. ¶14). In March, the registrars attempted to contact the registrants through the contact information available to them pursuant to the registrar-registrant agreements. *Id.* To date, however, no communications from the domain registrants have been received by the registrars, Microsoft or its counsel. *Id.*

Between February 27, 2010 and March 1, 2010 Microsoft made several attempts to provide notice of these proceedings and serve its complaint using the facsimile numbers associated with the Botnet Domains. (Docket no. 32, Ex. 2, ¶¶ 27-29). None of the facsimile numbers provided by the Doe Defendants is in operation. *Id.*

Since the entry of the temporary restraining order on February 22, 2010 and the subsequent preliminary injunction on March 10, 2010, the registrations for the Botnet Domains have been locked and the Botnet Domains have been removed from the zone files. These activities would also have given the registrants notice of this action and cause to investigate if no notice had been received. As previously found by the District Judge in granting the motion for a preliminary injunction, the methods used by Microsoft to serve the complaint and pleadings relating to the requests for injunctive relief were authorized by law, satisfy Due Process, satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify the defendants of this action. Since Microsoft has complied with the court's previous directives concerning service, the undersigned recommends a finding that the defendants have been provided with sufficient notice of this action.

Grounds for Entry of Default

Under Fed. R. Civ. P. 12(a), the Doe Defendants were required to file an answer or other responsive pleading with the Clerk at least by March 24, 2010, 21 days after the last email effectuating service was sent. No responsive pleading was filed by any Doe Defendant and Microsoft filed its request for entry of default (Docket no. 43) with a memorandum in support (Docket no. 47), and supporting affidavit (Docket no. 48) on July 12, 2010. Pursuant to an Order entered by the undersigned on August 6, 2010 (Docket no. 54), the Clerk of the Court entered a default as to each of the Does Defendants (Docket nos. 58-83, 87). Upon obtaining default, Microsoft filed its renewed motion for default judgment with its supporting declaration and noticed it for a hearing on September 3, 2010. (Docket nos. 84-86). The renewed motion for default judgment also incorporated by reference, *inter alia*, the arguments made in Microsoft's Application for an Emergency Temporary Restraining Order and Order to Show Cause re a

Preliminary Injunction ("Application") (Docket nos. 4, 5), its combined memorandum in support of the request for entry of default and motion for default judgment (Docket no. 47), and in the declarations of Gabriel Ramsey (Docket no. 48) and T.J. Campana (Docket no. 49). Pursuant to the District Judge's Order of March 10, 2010, Microsoft provided the Doe Defendants with copies of all of these pleadings by publication on noticeofpleadings.com, email or FedEx. (Docket nos. 84-86).

The undersigned magistrate judge recommends a finding that notice of this action was provided properly, that no defendant filed a responsive pleading in a timely manner, and that the Clerk properly entered a default as to the Doe Defendants.

Liability and Relief Sought

According to Fed. R. Civ. P. 54(c), a default judgment "must not differ in kind from, or exceed in amount, what is demanded in the pleadings." Because no responsive pleading was filed, the factual allegations in the complaint are deemed admitted.[3] *See* Fed. R. Civ. P. 8(b)(6). The relief sought in the complaint is "a preliminary and permanent injunction enjoining Doe Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or

[3] The complaint alleges that 273 domain names are part of the Waledac Botnet. Microsoft supplemented its request for a temporary restraining order to include an additional four domain names (Docket no. 14) that were controlled by the Doe Defendants. Microsoft withdrew its request as to one of the four additional domain names in its request for a preliminary injunction. (Docket no. 32) and the court entered a preliminary injunction as to 276 domain names (Docket no. 38). Even though the complaint has not been amended to include specifically those additional three domain names, those domain names are alleged to be controlled by the same Doe Defendants and notice has been provided as to the claims being made against those domain names.

performing any of the activity complained of herein or from causing any of the injury complained of herein." (Compl., Prayer for Relief, ¶ 1). Microsoft asserts that the only way to enjoin effectively the Doe Defendants' operation and propagation of the Waledac Botnet is to permanently deprive them of the Botnet Domains and transfer control of the domains to an entity that will ensure that they are not re-infected and revived as part of the Waledac Botnet. Microsoft is a natural candidate to be the entity in control of these domains because it is willing to bear the costs associated with ensuring that the domain registrations do not lapse, it has the technical expertise to ensure that the domains are not once again taken over by the Waledac Botnet, and it has no pecuniary interest in controlling those domains. Microsoft's only interest is in ensuring that those domains do not become part of the Waledac Botnet once again.

The complaint sets forth the following claims: (1) violations of Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (2) violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7704, (3) violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2701, (4) false designation of origin under the Lanham Act, 15 U.S.C. § 1125(a), (5) trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c)), (6) computer trespass, (7) unjust enrichment, and (8) conversion. Each claim will be discussed briefly below.

1. <u>Computer Fraud And Abuse Act</u>

The Computer Fraud and Abuse Act ("CFAA") penalizes, among other things, a party who: (i) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage (18 U.S.C. § 1030(a)(5)(C)); (ii) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer (18 U.S.C. § 1030(a)(2)(C)); or (iii) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer (18 U.S.C. § 1030(a)(5)(A)).

The parties controlling the Waledac Botnet intentionally access and send malicious code to Microsoft's and its customers' protected computers and operating systems without authorization in order to infect those computers and make them part of the botnet. The evidence submitted in support of this motion demonstrates that Microsoft and its customers are damaged by this intrusion. Performance of Microsoft's and its customers' computers is degraded due to the unauthorized intrusion, running of malicious code, collecting of personal information and carrying out of malicious conduct. Microsoft's Hotmail servers are burdened by the sending of an enormous amount of spam email to Microsoft's Hotmail accounts. This is precisely the type of activity that the CFAA is designed to prevent. *See, e.g., Physicians Interactive v. Lathian Systems, Inc.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting a temporary restraining order and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA). Indeed, some courts have observed that the CFAA was targeted at "computer hackers (*e.g.*, electronic trespassers)." *State Analysis, Inc. v. American Fin. Services. Assoc.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (citation omitted).

Further, spam emails sent by the Waledac Botnet to Hotmail users, by burdening Microsoft's servers supporting the Hotmail service and interfering with its goodwill, are actionable under the statute. *See, e.g., America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (defendant's spamming in violation of plaintiffs terms of service violated CFAA); *Hotmail Corp. v. Van$ Money Pie Inc.*, 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction under CFAA where defendant sent spam email to Hotmail subscribers without their authorization). As such, the undersigned recommends a finding that the Doe Defendants have violated the CFAA.

2. CAN-SPAM Act

The Controlling the Assault of Non-Solicited Pornography and Marketing Act ("the CAN-SPAM Act"), 15 U.S.C. § 7701 *et seq.*, prohibits, among other acts, initiation of a transmission of a commercial electronic mail message "that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Here, the Waledac Botnet automatically sends emails containing false "header" information (*i.e.* originating sender, IP address, etc.), making the emails appear to originate from user computers, false Hotmail addresses or other false addresses, thereby disguising their origin with the purpose of misleading recipients and evading detection. This is precisely what the CAN-SPAM Act prohibits. *See Aitken v. Communs. Workers of Am.*, 496 F. Supp. 2d 653, 667 (E.D. Va. 2007) (inaccurate "from" line and header information may violate CAN-SPAM). Thus, the undersigned recommends a finding that the Doe Defendants have violated the CAN-SPAM Act.

3. Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA") prohibits "intentionally accessing without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. The Waledac Botnet software, installed without authorization on infected computers, searches files such as emails and other files and extracts personal email addresses and other information from those sources. Once harvested, these email addresses become targets for spam email or are used for other malicious purposes. Obtaining stored electronic information in this way, without authorization, is a violation of the ECPA. *See Global Policy Partners, LLC*, 2009 U.S. Dist. LEXIS 112472, *8-13 (E.D. Va. 2009) (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc.*, 621 F. Supp. 2d at 317-318 (access of data on a computer without authorization actionable under ECPA). As such, the undersigned recommends a finding that the Doe Defendants have violated the ECPA.

4. False Designation Of Origin And Trademark Dilution

The Lanham Act prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person. 15 U.S.C. § 1125(a). The Waledac Botnet misleadingly and falsely causes the famous and distinctive Microsoft® and Windows® trademarks to be associated with malicious conduct carried out on users' computers through improper use of Microsoft's Windows operating system. Similarly, the Waledac Botnet misleadingly and falsely causes the famous and distinctive Hotmail® trademark to be the purported "source" of spam email and causes users of Hotmail to receive spam email. Further, the Waledac Botnet delivers fake and malicious antivirus software, misleadingly named "MS Antispyware 2009." This conduct causes confusion and mistake as to Microsoft's affiliation with such misconduct and creates the false impression that Microsoft is the origin. This activity is a clear violation of Lanham Act § 1125(a). *See, e.g., America Online v. IMS*, 24 F. Supp. 2d

548, 551-552 (E.D. Va. 1998) (spam email with purported "from" addresses including plaintiffs trademarks constituted false designation of origin).

The Lanham Act also provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark." 15 U.S.C. § 1125(c). Here, the Waledac Botnet's misuse of Microsoft's famous marks in connection with malicious conduct aimed at Microsoft's customers and the public dilutes these famous marks by tarnishment and by blurring of consumer associations with the marks. Again, this is a clear violation of Lanham Act § 1125(c). *See, e.g.*, *America Online*, 24 F. Supp. 2d at 552 (spam email with purported "from" addresses including plaintiffs trademarks constituted dilution). Thus, the undersigned recommends a finding that the Doe Defendants have violated sections 1125(a) & (c) of the Lanham Act.

5. Trespass To Chattels And Conversion

A trespass to chattels occurs "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," and "if the chattel is impaired as to its condition, quality, or value." *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451-452 (E.D. Va. 1998); *AOL v. IMS,* 24 F. Supp. 2d 548 (citing *Vines v. Branch*, 244 Va. 185,418 S.E. 2d 890, 894 (1992)) (trespass to chattels actionable in Virginia); *see also Barr v. City of Roslyn*, 2010 U.S. Dist. LEXIS 5541, *6-7 (E.D. Wash. 2010) (same). Similarly, "[a] person is liable for conversion for the wrongful exercise or assumption of authority over another's goods, depriving the owner of their possession, or any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights." *James River Mgmt. Co. v. Kehoe*, 2009 U.S. Dist. LEXIS 107847, *22-23 (E.D. Va. 2009); *Barr*, 2010 U.S. Dist.

LEXIS 5541 at *6-7 (under Washington law "conversion is the act of willfully interfering with any personal property without lawful justification, which causes the person entitled to possession to be deprived of that possession").

The unauthorized downloading of software and control over Microsoft's licensed Windows operating system software and the computers of customers interferes with and causes injury to the value of those properties. Thus, this conduct is an illegal trespass and constitutes conversion. *See Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting temporary restraining order and preliminary injunction where defendant hacked computers and obtained proprietary information holding "there is a likelihood that the two alleged attacks that [Plaintiff] traced to Defendants were designed to intermeddle with personal property in the rightful possession of Plaintiff"); *State v. Riley*, 121 Wash. 2d 22, 32 (Wash. 1993) (affirming conviction for "computer trespass" under Washington law for defendant's "hacking activity"); *Combined Ins. Co. v. West*, 578 F. Supp. 2d 822, 835 (W.D. Va. 2008) (conversion of "an electronic version of [a document]"); *In re Marriage of Langham*, 153 Wash. 2d 553, 566 (Wash. 2005) (conversion of intangible property). Likewise, unauthorized intrusion into Microsoft's servers providing the Hotmail service, by sending vast quantities of spam email, injures Microsoft's property and constitutes a trespass. *See, e.g., America Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (senders of spam e-mail committed trespass when they "caused contact with [plaintiff's] computer network ... and ... injured [plaintiff's] business goodwill and diminished the value of its possessory interest in its computer network."); *accord State v. Heckel*, 143 Wash. 2d 824, 834 (Wash. 2001) (spam email burdens possessory interest of computers, citing *AOL v. IMS*); *E.I. Dupont De Nemours &Co. v. Kolon Indus.*, 2009 U.S. Dist. LEXIS 76795, *25-26 (E.D. Va. 2009) (claim for conversion "based exclusively on the transfer of copies of electronic information"; noting that Virginia courts have demonstrated a distinct willingness to expand the scope of the doctrine of conversion in light of advancing technology). The undersigned recommends a finding that the Doe Defendants are liable for trespass to chattels and conversion.

6. Unjust Enrichment

The elements of a claim of unjust enrichment are (1) the plaintiff's conferring of a benefit on the defendant, (2) the defendant's knowledge of the conferring of the benefit, and (3) the defendant's acceptance or retention of the benefit under circumstances that "render it inequitable for the defendant to retain the benefit without paying for its value." *Nossen v. Hoy*, 750 F. Supp. 740, 744-45 (E.D. Va. 1990) (Virginia law); *Bailie Commc'ns Ltd. v. Trend Bus. Sys. Inc.*, 810 P.2d 12, 17-18 (1991) (same, under Washington law). Here, without authorization, the parties controlling the botnet have taken the benefit of Microsoft's servers, networks and email services, its licensed Windows operating system software and the computers of Microsoft's customers. They have done so by infecting these computers, collecting personal information and causing them to send and receive spam email. In doing so, the Doe Defendants have profited unjustly from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers. The Doe Defendants had knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers because they initiated the unauthorized use. Thus, it would be inequitable for the Doe Defendants to retain the benefit of their inequitable conduct and the undersigned recommends a finding that the Doe Defendants are liable for unjust enrichment.

Conclusion

For the foregoing reasons, the undersigned recommends that a default judgment be entered in favor of Microsoft Corporation and against the Doe Defendants and the 276 Botnet Domains. The undersigned further recommends that the terms of the preliminary injunction entered by the court on March 10, 2010 be converted into a permanent injunction, thereby enjoining the Doe Defendants and their officers, directors, principals, agents, servants, employees, successors, assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of in this action or from causing any of the injury complained of in this action and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of in this action or from causing any of the injury complained of in this action. The undersigned further recommends that the court enter an Order directing that VeriSign, Inc. transfer the 276 Botnet Domains listed on Appendix A attached hereto to a registrar of Microsoft's choosing that will then transfer the registration of the Botnet Domains to Microsoft. The undersigned also recommends that, upon the entry of a final order in this matter, the bond posted by Microsoft be released.

Notice to Parties

Microsoft is hereby directed to post a copy of these proposed findings of fact and recommendations on www.noticeofpleadings.com and to send a copy of these proposed findings of fact and recommendations to the defendants by electronic means and/or personal delivery as it has done in the past in accordance with the court's directives. Microsoft shall then file a notice with the court indicating that date and manner in which this service has been completed. The parties are hereby notified that objections to these proposed findings of fact and recommendations must be filed within fourteen (14) days of the filing of the notice by Microsoft that service of this proposed findings of fact and recommendations has been completed and a failure to file timely objections waives appellate review of the substance of these proposed findings of fact and recommendations and waives appellate review of any judgment or decision based on these proposed findings of fact and recommendations.

Entered this 17TH day of September, 2010.

/s/ JFA
John F. Anderson
United States Magistrate Judge
John F. Anderson
United States Magistrate Judge

Alexandria, Virginia

Appendix A

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellanews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhitechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com

61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com
77. adorepoem.com
78. adoresongs.com
79. bestadore.com
80. bestlovelong.com
81. funloveonline.com
82. youradore.com
83. yourgreatlove.com
84. orldlovelife.com
85. romanticsloving.com
86. adoresong.com
87. bestlovehelp.com
88. chatloveonline.com
89. cherishletter.com
90. cherishpoems.com
91. lovecentralonline.com
92. lovelifeportal.com
93. whocherish.com
94. worldlovelife.com
95. worshiplove.com
96. yourteamdoc.com
97. yourdatabank.com
98. alldatanow.com
99. alldataworld.com
100. cantlosedata.com
101. freedoconline.com
102. losenowfast.com
103. mingwater.com
104. theworldpool.com
105. wagerpond.com
106. beadcareer.com
107. beadworkdirect.com
108. bestcouponfree.com
109. bestmazdadealer.com
110. bluevalentineonline.com
111. buymazdacars.com
112. codecouponsite.com
113. deathtaxi.com
114. funnyvalentinessite.com
115. greatcouponclub.com
116. greatmazdacars.com
117. greatsalesavailable.com
118. greatsalesgroup.com
119. greatsalestax.com
120. greatsvalentine.com
121. greatvalentinepoems.com
122. macride.com

123. mazdaautomotiveparts.com
124. mazdacarclub.com
125. mazdaspeedzone.com
126. netcitycab.com
127. petcabtaxi.com
128. smartsalesgroup.com
129. superpartycab.com
130. supersalesonline.com
131. thecoupondiscount.com
132. themazdacar.com
133. themazdaspeed.com
134. thevalentinelovers.com
135. thevalentineparty.com
136. wirelessvalentineday.com
137. workcaredirect.com
138. workhomegold.com
139. worklifedata.com
140. yourcountycoupon.com
141. yourmazdacar.com
142. yourmazdatribute.com
143. yourvalentineday.com
144. yourvalentinepoems.com
145. againstfear.com
146. antiterroralliance.com
147. antiterroris.com
148. antiterrornetwork.com
149. bayhousehotel.com
150. bestblogdirect.com
151. bestbreakingfree.com
152. bestjournalguide.com
153. bestlifeblog.com
154. bestusablog.com
155. blogginhell.com
156. blogsitedirect.com
157. boarddiary.com
158. breakingfreemichigan.com
159. breakinggoodnews.com
160. breakingkingnews.com
161. breakingnewsfm.com
162. breakingnewsltd.com
163. debtbgonesite.com
164. easyworldnews.com
165. extendedman.com
166. farboards.com
167. fearalert.com
168. globalantiterror.com
169. gonesite.com
170. longballonline.com
171. mobilephotoblog.com
172. photoblogsite.com
173. residencehunter.com
174. terroralertstatus.com
175. terrorfear.com
176. terrorismfree.com
177. themostrateblog.com
178. tntbreakingnews.com
179. urbanfear.com
180. usabreakingnews.com
181. yourbreakingnew.com
182. yourlength.com
183. yourlol.com
184. yourwent.com

185. bakeloaf.com
186. chinamobilesms.com
187. coralarm.com
188. downloadfreesms.com
189. freecolorsms.com
190. freeservesms.com
191. fryroll.com
192. goldfixonline.com
193. lastlabel.com
194. miosmsclub.com
195. moneymedal.com
196. nuovosms.com
197. screenalias.com
198. smsclubnet.com
199. smsdiretto.com
200. smspianeta.com
201. tagdebt.com
202. virtualesms.com
203. wealthleaf.com
204. yourbarrier.com
205. discountfreesms.com
206. eccellentesms.com
207. freesmsorange.com
208. ipersmstext.com
209. morefreesms.com
210. nuovosmsclub.com
211. primosmsfree.com
212. smsinlinea.com
213. smsluogo.com
214. superioresms.com
215. 4thfirework.com
216. biumer.com
217. entrank.com
218. fireholiday.com
219. fireworksholiday.com
220. fireworksnetwork.com
221. fireworkspoint.com
222. freeindependence.com
223. gemells.com
224. handyphoneworld.com
225. happyindependence.com
226. holidayfirework.com
227. holidaysfirework.com
228. holifireworks.com
229. interactiveindependence.com
230. miosmschat.com
231. movie4thjuly.com
232. moviefireworks.com
233. movieindependence.com
234. movies4thjuly.com
235. moviesfireworks.com
236. moviesindependence.com
237. outdoorindependence.com
238. smophi.com
239. superhandycap.com
240. thehandygal.com
241. video4thjuly.com
242. videoindependence.com
243. yourhandyhome.com
244. yusitymp.com
245. aweleon.com
246. bedioger.com

247. bicodehl.com
248. birdab.com
249. cismosis.com
250. crucism.com
251. cycloro.com
252. encybest.com
253. favolu.com
254. framtr.com
255. frostep.com
256. gumentha.com
257. hindger.com
258. hornalfa.com
259. noloid.com
260. nonprobs.com
261. oughwa.com
262. painkee.com
263. pantali.com
264. pathoph.com
265. prerre.com
266. purgand.com
267. rascop.com
268. sodanthu.com
269. specipa.com
270. tabatti.com
271. tatumen.com
272. thingre.com
273. tobeyew.com
274. broadwo.com
275. houreena.com
276. cyanian.com